**What is claimed is:**

**1.** A method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, the method comprising:

(a) receiving a request for an access permission security profile on behalf of a network user;

(b) authenticating the request;

(c) creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object; and

(d) securely transmitting the access permission security profile to the network user over the network.

**2.** The method of claim **1**, wherein the creating step comprises:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities;

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

**3.** The method of claim **2**, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

**4.** A method for providing decryption capabilities to a plurality of network users over a decentralized public network, the method comprising:

(a) receiving a request for decryption capabilities on behalf of a network user;

(b) authenticating the request;

(c) creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object;

(d) receiving from the user information associated with the encrypted object;

(e) generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object; and

(f) securely transmitting the cryptographic key to the network user over the network.

**5.** The method of claim **4**, wherein the creating step includes:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities;

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

**6.** The method of claim **5**, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

**7.** A method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users, the method comprising:

(a) creating a computer representable data object including one or more embedded objects;

(b) selecting one or more embedded objects of the data object to be encrypted;

(c) encrypting the selected embedded objects;

(d) creating one or more access permission credentials;

(e) assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object;

(f) authorizing the user; and

(g) transmitting the data object over the network.

**8.** The method of claim **7**, wherein the information is digital content.

**9.** The method of claim **7**, wherein the authorizing step includes:

(i) receiving a request for an access permission security profile on behalf of a network user;

(ii) authenticating the request; and

(iii) securely transmitting the security profile to the network user over the network.

**10.** The method of claim **7**, wherein the authorizing step includes:

(i) sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network;

(ii) receiving the request at the central server system;

(iii) authenticating the request; and

(iv) securely transmitting the security profile from the server system to the network user over the network.

**11.** The method of claim **7**, wherein the authorizing step is automatic and based upon the user's possession of a security profile token.

**12.** The method of claim **7**, wherein the encrypting step comprises:

(i) identifying a group of network users who are to be allowed access to a data object to be encrypted;

(ii) generating an appropriate cryptographic credential key from a set of credential categories, said credential key relating to the group of network users;

(iii) generating a cryptographic working key from at least a domain component, a maintenance component, and a pseudorandom component;

(iv) encrypting the data object with the working key;

(v) encrypting the pseudorandom component with the credential key; and

(vi) associating the encrypted pseudorandom component to the encrypted data object.

**13.** The method of claim **7**, wherein the access permission security profile is created by:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities;

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key; and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code.

**14.** The method of claim **13**, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

**15.** The method of claim **1**, **4** or **9**, wherein the request is initiated in-band by the network user over the network.

**16.** The method of claim **1**, **4**, **9**, **10**, or **11**, wherein the access permission security profile is in the form of a token that is adaptable to expire.

**17.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of biometric identification.

**18.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of a hardware token.

**19.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of a software token.

**20.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of a user password.

**21.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of a record of time at which the request was made.

**22.** The method of claim **1**, **4**, **9**, or **10**, wherein the authenticating step includes the use of a record of the user's physical location.

**23.** A method for controlling access to a secured system, the method comprising:

(a) selecting one or more portions of the system to be secured;

(b) creating one or more groups of system users, said groups defining which users are to be allowed access to which secured portions of the system;

(c) establishing one or more access codes for each group;

(d) assigning the access codes to the secured portions of the system, wherein each access code is adapted to be combined with other components to form a key for controlling access to one or more secured portions of the system.

(e) securing the access codes; and

(f) distributing over a decentralized public network the secured access codes to users of the system who are to be allowed access to one or more of the selected portions of the system.

**24.** The method of claim **23**, wherein the secured system is a physical system.

**25.** The method of claim **23**, wherein the secured system is a computer network.

**26.** The method of claim **23**, wherein the secured access codes are at least partially secured through biometric identification.

**27.** The method of claim **23**, wherein the secured access codes are at least partially secured through a soft token.

**28.** The method of claim **23**, wherein the secured access codes are at least partially secured through a hardware token.

**29.** The method of claim **23**, wherein the secured access codes are at least partially secured through a password.

**30.** The method of claim **23**, wherein the secured access codes are at least partially secured by the use of a record of time at which the request was made.

**31.** The method of claim **23**, wherein the secured access codes are at least partially secured by the use of a record of a user's physical location.

**32.** A method for administering cryptographic capabilities over a decentralized public network to a plurality of network users, the method comprising:

(a) identifying one or more groups of network users for defining which users are to be provided with cryptographic capabilities;

(b) creating a member account for each network user in each group;

(c) performing administrative tasks associated with maintaining the member accounts in a single database;

(d) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key;

(e) creating one or more security profiles for each network user in each group, wherein each security profile is stored in the user's member account and contains at least one access code;

(f) generating a member token relating to each security profile;

(g) securing the security profiles and related member tokens; and

(h) distributing the member tokens over the network to individual network users upon authenticated request and according to each individual user's security profile.

**33.** The method of claim **32**, wherein the establishing step further includes creating credentials and encryption algorithms for defining role-based access permissions.

**34.** The method of claim **32**, wherein the performing step is accomplished remotely over the decentralized public network.

**35.** The method of claim **32**, wherein the creating steps are accomplished remotely over the decentralized public network.

**36.** The method of claim **32**, wherein the creating and distributing steps are accomplished automatically.

**37.** The method of claim **32**, wherein the administrative tasks include reporting member activities, system events and billing activities.

**38.** The method of claim **32**, wherein the administrative tasks include adding member accounts, removing member accounts, and updating member accounts.

**39.** The method of claim **32**, wherein each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain.

**40.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through biometric identification.

**41.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through a soft token.

**42.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through a hardware token.

**43.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through a personal identification number.

**44.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through the use of a record of the time.

**45.** The method of claim **32**, wherein the security profiles and member tokens are at least partially secured through the use of a record of a user's physical location.

**46.** A centralized security management system for administering and distributing cryptographic capabilities over a decentralized public network, the system comprising:

(a) a set of server systems;

(b) a set of member domains, wherein each member domain is maintained on at least one of the server systems;

(c) a set of system maintenance tasks associated with maintaining the set of member domains;

(d) one or more system administrators for performing the set of system maintenance tasks;

(e) a set of members, wherein each member is associated with at least one member domain via a member account;

(f) a set of member security profiles, wherein each security profile is uniquely associated with a member account and provides cryptographic capabilities to the member associated with the member account;

(g) a set of administrative tasks associated with maintaining the set of member accounts; and

(h) a set of domain administrators for performing the administrative tasks remotely over the network.

**47.** The system according to claim **46**, wherein each member account includes means for member identification and authentication.

**48.** The system according to claim **46**, wherein at least one server system includes means for member identification and authentication.

**49.** The system according to claim **46**, wherein each member account is associated to a single member.

**50.** The system according to claim **46**, wherein the set of administrative tasks includes reporting and accounting tasks relating to each member account.

**51.** The system according to claim **46**, wherein the administrators are divided into hierarchically structured groups according to different levels of the administrative tasks.

**52.** A centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, the system comprising:

(a) a plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network;

(b) a set of server systems for managing the distribution of the member tokens;

(c) means for requesting a member token from at least one server system;

(d) a set of client systems, wherein each client system includes

(i) means for receiving the requested member token, and

(ii) means for utilizing the cryptographic capabilities provided by said member token; and

(e) means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network.

**53.** The system of claim **52**, wherein each client system further includes user authentication means.

**54.** The system of claim **52**, wherein the means for requesting a member token resides on each client system.

**55.** The system of claim **52**, wherein means for authenticating a user resides on at least one server system.

**56.** The system of claim **52,** wherein managing the distribution of the member tokens includes dynamic updating of the member tokens.

**57.** The method of claim **1**, **4**, **7**, **23**, **32**, **46**, or **52**, wherein the decentralized public network is the Internet.

**58.** The method of claim **1**, **4**, **7**, **23**, **32**, **46**, or **52**, wherein the decentralized public network is a cellular phone network.